Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matter of	)	
	)	
Spectrum Needs of Emergency	)	WT Docket No. 05-157
Responders	)	FCC 05-80
	)	

COMMENTS OF LUCENT TECHNOLOGIES, INC.

Charles B. Mathias
Lucent Technologies, Inc.
1100 New York Avenue, NW
640 West Tower
Washington, DC 20005
(202) 312-5908
cbmathias@lucent.com

April 28, 2005

TABLE OF CONTENTS

SUMMARY

Section 7502 of the Intelligence Reform and Terrorism Prevention Act of 2004 outlines a Congressional initiative to address some unintended oversights that impact the extended public safety community's ability to communicate and share large amounts of complex information in the field. The initiative seeks to assess current telecommunications needs of the public safety community and address whether the deployment of a *nationwide, interoperable, broadband mobile* communications network would improve the information sharing needs of the first responder community. The initiative also seeks to assess the role of *commercially available technologies* to deliver mission critical communications capabilities to this community.

Significant work is already under way to ensure that today's communications stovepipes are integrated in a coherent fashion to better serve the country's needs. However, the focus of these efforts is primarily on narrowband (voice) communications. Lucent Technologies believes that there should be a similar focus on the creation of an interoperable, National Mobile Broadband Network ("NMBN") that is available to America's extended emergency response community.

Lucent believes that a national mobile broadband system should, at a minimum, provide for real-time, high speed, *highly secure* wireless access and transmission of remote computer applications and files; rapid messaging, including e-mail, free-form text, and file transfers; constantly updated personnel and equipment location and status data; aerial video for major events and

disaster response coordination; transmission and reception of high-resolution digital images (including maps, floor plans and complex diagrams); satellite connectivity of disaster "hot-spots"; bandwidth on demand; and prioritization of services.

The NMBN must be available where and when America's National Responders need it. It must be reliable, and it must be secure and capable of supporting in the field the ever-increasing specialized IP-based applications that are being developed to support the National Responder ("NR") community.

Lucent Technologies believes that the NR community should be defined to include up to 8 to 10 million public safety users, including those from the utilities, public health and critical infrastructure sectors, the military and national security communities, and disaster relief agencies. Providing interoperable mobile broadband capabilities will lead to efficiencies and new ways of working similar to the changes that are taking place today in the commercial sector.

To bring these benefits to this extended community, Lucent envisions the *creation and deployment of a dedicated networ*k that would aggregate the *full NR community into a single user class*. The national network would be comprised of discrete regional operations *utilizing commercial broadband wireless technology* for the platform in the *lowest possible available spectrum*. While Lucent is conducting an ongoing analysis, Lucent believes that approximately *10 to 15 MHz of spectrum* should be sufficient to meet the needs of an expanded NR community.

The creation of a dedicated, secure, broadband mobile network will provide to America's National NRs a communications platform on a par with the most advanced commercial users. It will offer a ubiquitous communications infrastructure capable of acting as a universal transport layer for information sharing, as a gateway to private and public networks and as a means of providing connectivity or backhaul for other security-related networks. The deployment of a national network is a large undertaking--- but it is an undertaking that *can* and *must* be achieved to meet the communications requirements of a NR community that is asked to meet ever-greater challenges in protecting the needs of all Americans.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matter of	)	
	)	
Spectrum Needs of Emergency Responders	))	WT Docket No. 05-157 FCC 05-80
	)	

COMMENTS OF LUCENT TECHNOLOGIES, INC.

Lucent Technologies, Inc. ("Lucent") respectfully submits the following comments in response to the public notice issued by the Federal Communications Commission ("FCC") in the above-captioned proceeding.[1]

I. THE CONGRESSIONAL REQUEST FOR STUDIES REFLECTS THE NATIONAL IMPERATIVE TO FIND A SECURE WAY TO GET LARGE AMOUNTS OF COMPLEX INFORMATION TO THE FIELD, IN THE CONTEXT OF AN ONGOING THREAT

The Congressional request for studies outlined in Section 7502 of the Intelligence Reform Act[2] is aimed at determining whether the creation of a dedicated mobile broadband capability using commercial technologies for the NR community would enhance the nation's ability to respond to incidents. The National Strategy for Homeland Security outlines a vision to "strive to create a fully integrated national emergency response system that is adaptable enough to deal with any terrorist attack, no matter how unlikely or catastrophic, as well as

[1] *FCC Requests Comment on Spectrum Needs of Emergency Response Providers: Input Required for FCC Report Mandated by the Intelligence Reform and Terrorism Prevention Act of 2004*, WT Docket No. 05-157, Public Notice (rel. Apr. 28, 2005) (FCC 05-80) ("*Request for Comments*").

[2] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638, § 7502 (2004) ("Intelligence Reform Act").

all manner of natural disasters."[3] Section 7502 outlines an integrated, comprehensive initiative to address unintended oversights that impact the ability of the full, extended public safety community to communicate with each other and the types of information that they would be able to share. This initiative has the distinction of addressing, on three separable but interrelated levels, the information-sharing needs of the entire public safety community in order to assure that a new alternative is provided for those that serve the protection, safety and security interests of this country. This initiative, upon completion of the studies requested by Congress, will address whether the deployment of a nationwide interoperable broadband mobile communications network, under these revised parameters, could serve the information-sharing needs of "Federal, State, regional, and local governmental and nongovernmental public safety, homeland security, and other emergency response personnel."[4] In addition, the studies seek to assess whether the use of *commercial wireless technologies* to deliver this capability is practicable under those circumstances, and whether Congress should grant an additional allocation of spectrum to serve the extended universe of emergency service providers. Conclusions from this assessment may lead to recommendations for the development of such a NMBN for this

[3] *The National Strategy for Homeland Security*, Office of Homeland Security, July 2002, at 42, *available at*: <http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf> ("*National Strategy for Homeland Security*").

[4] Intelligence Reform Act § 7502(b)(1).

extended public safety community, as many, including Lucent Technologies, have advocated.[5]

II. MEETING THIS INFORMATION-SHARING IMPERATIVE REQUIRES A NATIONAL, INTEROPERABLE, MOBILE, BROADBAND SYSTEM AVAILABLE TO EMERGENCY RESPONDERS

The National Response Plan ("NRP") assists in the important homeland security mission of preventing terrorist attacks within the United States; reducing the vulnerability to all natural and manmade hazards; and minimizing the damage and assisting in the recovery from any type of incident that occurs.[6] The NRP is an all-discipline, all-hazards plan that establishes a single, comprehensive framework for the management of domestic incidents. However, national policy regarding the use of spectrum or shared use of communications infrastructure by both FCC and National Telecommunications and Information Administration ("NTIA") constituent communities is not currently treated in a similarly comprehensive manner. With the study language outlined in Section 7502 of the Intelligence Reform Bill, Congress appears interested in fast-tracking a number of the recommendations outlined in the "Presidential Spectrum Policy Direction to

[5] *See, e.g.,* "Protecting Homeland Security: A Status Report on Interoperability Between Public Safety Communications Systems," Testimony of Gary Grube, Corporate Vice President and Chief Technology Officer, Commercial, Government and Industrial Solutions, Motorola, Inc., at Hearing Before the U.S. House of Representatives Subcommittee on Telecommunications & the Internet (June 23, 2004); *See also* "Spectrum for Public Safety Users," Testimony of Gary Grube, Corporate Vice President and Chief Technology Officer, Commercial, Government and Industrial Solutions, Motorola, Inc., at Hearing Before the United States Senate Committee on Commerce, Science & Transportation (Sept. 8, 2004).

[6] *National Response Plan*, Department of Homeland Security, December 2004, *available at*: <http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf> ("*National Response Plan*").

Ensure the Protection of Critical Government Spectrum Users and Services."[7] In particular, the directives outlined in the Congressional study language seek to have the responsible parties (the FCC, NTIA, and Department of Homeland Security ("DHS"), with input from all potential user communities) recognize and address the spectrum issues associated with aggregating this extended emergency response user community. The Congressional directive, in its current state, is a direct extension of key recommendations coming from the Presidential Spectrum Direction and the creation of a NMBN as a means of sharing information is a logical implementation of those recommendations.

Significant effort is underway to ensure that the countless stovepipes of radio systems are integrated into a more coherent fashion under the Federal leadership of SAFECOM. Their focus however, remains primarily in the integration of *narrowband* communication systems to enhance (voice) communication capabilities. These "stovepipe" systems represent more than $18.3 B[8] in assets across this country, and are assets that cannot and should not be replaced. However, given the increasing importance of IP-based, data-driven communications, Lucent believes that a national broadband network must be deployed to ensure that tools, applications, and ultimately, information -- can be accessed by, shared within, and used by, this community.

[7] The Presidential Directive was issued in November 2004 in response to recommendations from the Federal Government Spectrum Policy Task Force in its two reports entitled *Spectrum Policy for the 21st Century – The President's Spectrum Policy Initiative*.

[8] "LMR Replacement Cost Study Report," Public Safety Wireless Network, June 1998, *available at*: <http://www.safecomprogram.gov/NR/rdonlyres/B69361FA-9AC6-4126-B971-83DF30FED932/0/lmr_coststudy.pdf>.

A. Secure and Highly Reliable Access Requires a Dedicated and Interoperable Network

The technical requirements for data by various NR communities share common attributes, and are characterized in part by the following characteristics:[9] real-time, high-speed wireless access and transmission of remote computer applications and files; rapid messaging, including e-mail, free-form text, and file transfers; constantly updated personnel and equipment location and status data; aerial video for major events and disaster response coordination; transmission and reception of high-resolution digital images (including maps, floor plans and complex diagrams); satellite connectivity of disaster "hot-spots"; bandwidth on demand; prioritization of services; and highly secure (encrypted) communications, as may be required. The security and availability requirements across this constituency also share comparable characteristics. These requirements generally fall into the following areas:[10]

1) *Confidentiality:* information is seen and accessed only by intended recipients, and created primarily through the use of protocols that use encryption;

2) *Integrity:* information received is the same information transmitted by the originator, unchanged;

[9] *See* "Introduction to the Project MESA Statement of Requirements," *available at*: <http://www.projectmesa.org/MESA_SoR/SoR.htm> ("MESA SoR").

[10] *See Pentagon Area Common Information Technology (IT) Wireless Security Policy*, September 2002, attached to Office of the Secretary of Defense Memorandum for Secretaries of the Military Departments, *et al.* (Sept. 25, 2002), *available at*: <http://www.defenselink.mil/nii/org/cio/doc/it-wireless-policy-092502.pdf>.

3) *Authentication:* identifies an individual or computer (device) to ensure access to information is authorized;

4) *Non-repudiation:* ensures that an individual cannot deny sending or receiving information; and

5) *Availability:* Ensures that information (voice, video, and data) and supporting service resources (*e.g.*, server, local networking infrastructures, and transport medium) are operating when needed.

Operational requirements for public safety operations are generally more stringent than commercial operations and reflect the need for:

1) *Enhanced Coverage:* Must cover ubiquitously those areas that must be served, rural wilderness areas as well as interiors of buildings and systems (*e.g.*, subways) in dense urban areas;

2) *Availability:* Must be able to handle high-volume surges in communications when and where an emergency occurs, which implies system capacity over-provisioning; and

3) *Reliability:* Services used for the control, operation and maintenance of critical infrastructure companies, utilities or other emergency response services must have a very high level of reliability, which implies higher levels of redundancy, diversity and recovery within the network. In short, the unique needs of this extended NR community must be accommodated by a dedicated, secure, mobile broadband network.

B. Current Emergency Protocols Must Be Capable of Communicating Large Amounts of Data Immediately to All Response Personnel; Therefore, the System Must Be Interoperable

The ability to communicate before, during, and after public emergencies is central to the public safety community's ability to prepare for, and respond to, such incidents. Homeland security planners recognized the importance of good communications as they drafted the Bush administration's *National Strategy for Homeland Security*. The strategy elaborates a national vision to "strive to create a fully integrated national emergency response system that is adaptable enough to deal with any terrorist attack, no matter how unlikely or catastrophic, as well as all manner of natural disasters."[11] The DHS is to "consolidate federal response plans and build a national system for incident management [with the] aim to ensure that leaders at all levels of government have complete incident awareness and can communicate with and command all appropriate response personnel."[12] Responsibility falls on Federal, state, and local governments to "ensure that all response personnel and organizations – including the law enforcement, military, emergency response, health care, public works, and environmental communities – are properly equipped, trained, and exercised to respond to all terrorist threats and attacks in the United States."[13] "This national

[11] *National Strategy for Homeland Security*, *supra* note 3*, at 42.*

[12] *Id.*

[13] *Id.*

vision sets forth a set of broad objectives in terms of future capabilities for a national, integrated public safety communications system. "[14]

C. Emergency Service Providers Need to Share Information That Requires Broadband Transmissions

The creation of a NMBN would not replace current private voice and/or dispatch networks used by the NR community. Rather the NMBN is designed to act as a means to provide in-field data access to the "trusted information network."[15] Through the creation of a NMBN, the government will go a long way to create a "dynamic, distributed network for sharing and analysis."[16] The creation of this dedicated broadband network would enable first responders to utilize critical applications that are currently available but not accessible via voice or on the slower speed networks currently in use. These applications include mapping/location based services, video streaming of security or incident scene, digital image transfers, large file transfers, biometric information, and bio-terrorism detection and response information. This data already exists—but there is no consistent, secure and dedicated means to send this information to the field, or to send this type of information from the field to a command environment. These applications are all being built in the IP domain, and IP

[14] *What Should We Know? Whom Do We Tell? Leveraging Communications and Information to Counter Terrorism and Its Consequences*, Chemical and Biological Arms Control Institute (CBACI), Project Report, December 2002, *available at*: <http://www.cbaci.org/pubs/reports/what_should_we_know/>.

[15] *See Creating a Trusted Information Network for Homeland Security*, Second Report of the Markle Foundation Task Force, December 2003, *available at*: <http://www.markletaskforce.org/reports/TFNS_Report2_Master.pdf> (emphasis added).

[16] *Id.* At 7.

Access provides the mechanism for sending and receiving such information to those who will act upon it.

Ongoing government information-sharing initiatives will remain isolated if there is no secure way to extend mission-critical, data-rich information to the field. The growing role of information-sharing in both the public safety and homeland security arena is exemplified by a number of initiatives currently being funded at all levels of government in this country. Three initiatives, in particular, serve as indications of the growing importance of this form of data- or information-sharing to this community.

The DHS's Chimera initiative will culminate in an integrated system designed to provide both DHS and the Department of State with real-time access to law enforcement and intelligence information concerning aliens.[17] Current funding of this initiative has already exceeded $1B in FY2002-2004 .[18] A comparably sized initiative, referred to as the Global Information Grid ("GIG"), is designed to provide authorized users with a seamless, secure, and interconnected information environment, meeting real-time and near real-time needs of both the war-fighter and the business user. It will use commercial technologies augmented to meet DoD's mission-critical user requirements. The program's vision implies a fundamental shift in information management,

[17] The term "Chimera system" refers to "the interoperable electronic data system required to be developed and implemented by section 202(a)(2) [8 U.S.C. § 1722(a)(2)]." 8 U.S.C. § 1701(3).

[18] *Department of Homeland Security: Budget in Brief* (FY 2004), *available at*: <http://www.dhs.gov/interweb/assetlibrary/FY_2004_BUDGET_IN_BRIEF.pdf> ("*DHS Budget in Brief*").

communication, and assurance,[19] and DOD plans to spend at least $21 billion through 2010 to build a core GIG capability.[20]

The third initiative, to support the sharing of information among and between the Critical Infrastructure ("CI") Sectors, is a DHS initiative to promote collaboration and coordination among the CI Information Sharing & Analysis Centers ("ISAC") ultimately to support information analysis and infrastructure protection efforts. The current FY2004 budget for the ISAC program is $829 million.[21]

These initiatives, when implemented, will ultimately provide the ability to access and analyze information from all government and non-government entities, to associate threat information with infrastructures, national assets and people -- and to share threat analysis with federal, state, local government and law enforcement agencies and private sector entities.

Despite the tens of billions of dollars associated with creating an environment of information sharing evidenced by these three initiatives, there is *no* organized plan or approach to ensure that this information can be sent or received in a secure and dedicated manner to individuals *in the field* -- where the information can be used effectively to save people, evidence, property or the

[19] "Global Information Grid," National Security Agency, *available at*: <http://www.nsa.gov/ia/industry/gig.cfm>.

[20] *See Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation*, United States Government Accountability Office Report to the Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services, House of Representatives, July 2004, *available at*: <http://www.gao.gov/new.items/d04858.pdf>.

[21] *See DHS Budget in Brief*, *supra* note 18.

environment. It is this oversight that Congress seeks to address in the studies it has requested.

D. Access in the Field Must Be Mobile, Hence the Need for Spectrum

Both public and private sector interests have addressed the need for a mobile broadband platform for homeland security in recent years. In filings before the FCC, Northrop Grumman petitioned the Commission to consider providing an additional allocation of spectrum for broadband applications.[22] In that petition, Northrop Grumman IT Systems urged the FCC to identify spectrum to establish *a nationwide, IP-based, interoperable communications network that will support broadband services for homeland security purposes*.

The Utility Telecommunications Council, in testimony before The House Committee on Energy and Commerce, outlined the lack of dedicated spectrum for critical infrastructures, the crucial importance of communications capability between themselves and other public safety entities, *and the need for a nationwide emergency communications network.*[23]

[22] Petition for Rulemaking of Northrop Grumman Information Technology (Apr. 21, 2003). The Wireless Telecommunications Bureau and Office of Engineering Technology subsequently dismissed the petition. *See* Letter from J. B. Muleta and E. J. Thomas to M. W. Grady, DA 03-2940 (Sept. 24, 2003).

[23] "The Spectrum Needs of Our Nation's First Responders," Testimony of Stephen Carrico, Director of Communications and Business Development, Wisconsin Public Service Corporation, on Behalf of the United Telecom Council, Prepared for the U.S. House of Representatives Subcommittee on Telecommunications & the Internet (June 11, 2003), *available at*: <http://energycommerce.house.gov/108/Hearings/06112003hearing951/Carrico1535print.htm>.

E. A Broad Group of National Responders Requires Access

The Congressional studies outlined in Section 7502 of the Intelligence Reform Act contemplate the creation of a NMBN that could be used by "Federal, State, regional, and local governmental and nongovernmental public safety, homeland security, and other emergency response personnel."[24] Lucent Technologies believes this extended community constitutes the NR community described above and estimates its size to be approximately 8-10M users.

In aggregate, Lucent Technologies believes the community of users would include individuals from countless government, public and private agencies: These users include traditional Public Safety (Fire, Police, EMS); Utilities/Public Works; Military Support (US North COM, National Guard); Federal Agencies (Port Security, Emergency Management, Public Health, etc.); Critical Infrastructure Providers (Financial Services, Energy Services, Transportation); National Security and Emergency Preparedness Users; State, Regional, Municipal and Tribal Personnel; Hospitals, Clinics; and Governmental and Non-Governmental Response Entities and volunteers.

Project MESA, an international collaborative for the coordination and development of next-generation high-mobility wireless broadband services,[25] reflects this inclusive approach in its Statement of Requirements, and is intended to be more in line with the 1997 amendments to the Communications Act[26] rather

[24] Intelligence Reform Act § 7502(b)(1).

[25] *See* Mesa SoR, *supra* note 9.

[26] In 1997 amendments to the Communications Act of 1934, Congress defined public safety services as "services--- (A) the sole or principal purpose of which is to protect the safety of life, health of property; (B) that are provided (i) by

than more restrictive versions generally used in the context of funding initiatives. Lucent contends that *applying the broadest possible definition to this user community is the approach that best meets the objectives of this NMBN initiative*. When viewed in the various contexts of: a) the traditional public safety community; and b) extended "first responder" definitions[27] through the broadest incorporation of the initiatives cited above, it is clear that Congress intends to treat this public safety enterprise as a whole, and recognizes that current policies separating NTIA user communities and FCC user communities are not fully within either agency's authority to resolve individually.

F. Corollary Benefits of Widespread, Interoperable Broadband Public Safety Service Include Efficiency and Improved Ability to Carry Out Missions

Providing mobile broadband[28] communications capabilities to the expanded NR community is consistent with Administration policy to provide

State or local government entities; or (ii) by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services; and (C) that are not made commercially available to the public by the provider." 47 U.S.C. § 337 (f)(1).

[27] As outlined in the "Homeland Security Presidential Directive/Hspd-8": "The term 'first responder' refers to those individuals who in the early states of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations." "Homeland Security Presidential Directive/Hsppd-8," § 2(d) (Dec. 17, 2003), *available at*: <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html>.

[28] The FCC defines broadband as an "advanced telecommunications capability" that has "the capability of supporting, in both the provider-to-consumer (downstream) and the consumer-to-provider (upstream) directions, a speed (in

universal access to broadband technologies and provides a platform for secure information-sharing within this NR user community.

Mobile broadband access is beginning to change the way consumers and businesses acquire and exchange information, and operate their daily business outside their traditional offices. Lucent believes the NR community should also have the opportunity to receive information while in the field, where the information is needed, communicated, and acted upon. Fundamental shifts in the provisioning of public interest services have been associated with the surge in IP applications and broadband transport mechanisms, particularly in the areas of tele-medicine, distance-learning and remote sensor applications. These benefits stemmed from the availability of standards-based (IP) platforms and robust commercial transport networks. Moreover, mobile broadband access for this particular NR user class could provide significant opportunities to restructure and reduce the time and costs associated with accomplishing routine, as well as mission-critical tasks.

Efficiencies associated with more time-sensitive deployment of public safety personnel, reduced time in reaching the scene of an incident coupled with increased information about the situation, and more efficient records management through on-site officer incidence reports alone would be significant.

technical terms, 'bandwidth') in excess of 200 kilobits per second (kbps) in the last mile. This rate is approximately four times faster than the Internet access received through a standard phone line at 56 kbps." *Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996*, Report, CC Docket No. 98-146, 14 FCC Rcd 2398, ¶ 20 (1999).

For example, Lucent's study of the early operational efficiencies of the El Paso, TX police department indicate that the daily use of their electronic incident report form saved 30 minutes of process time (or $180/day). This translates into a savings of $65K per year per officer. When multiplied by the estimated 8-10M users of the NR community, the savings overall could be in the tens of billions of dollars per year -- efficiencies that will be felt immediately by municipalities, states and federal agencies. More important, however, is the enhanced effectiveness of operations achieved by having a consistent means to leverage existing information on a daily, routine basis in the execution of one's mission. Consistent with the SAFECOM Interoperability Continuum,[29] daily use throughout the region can lead to comprehensive training and exercises, consistent with the National Incident Management System and Integrated SOPs. This level of ubiquity provides for continuous improvement in daily operations, pre-incident planning and coordination, enhanced situational awareness during an incident, and reinforces the strength of the public safety communications network as a whole.

III. A DEDICATED, NATIONAL, MOBILE BROADBAND SYSTEM DOES NOT EXIST TODAY

A. There Is No Dedicated Access in the Field to Broadband Data and Applications

The vast majority of NRs have no dedicated access to mobile broadband capabilities. Inadequate and unreliable wireless communication is a serious

[29] *SAFECOM Interoperability Continuum*, Department of Homeland Security, *available at*: <http://www.safecomprogram.gov/NR/rdonlyres/72E16B22-6928-4676-A82A-B6858E7974FA/0/InteroperabilityContinuum.pdf> ("*Interoperability Continuum*").

issue plaguing public safety agencies. In many instances, agencies lack the technology necessary to perform their mission critical duties. In addition to interoperability problems, traditional public safety wireless systems lack the required security, spectral efficiency, voice quality and high-speed data capabilities. Furthermore, these systems are based on technology dominated by a very small vendor community. This fact, combined with today's relatively closed market due to spectrum channelization constraints, limits innovation and competition, forcing the public safety community to accept out-dated capabilities at a high price. These narrowband systems are currently augmented by commercial low-speed data services using Cellular Digital Packet Data ("CDPD"), and in some cases, by commercial cellular voice services. Current data applications for this community range in the 19.2 kbps range, and in the absence of a dedicated broadband spectrum allocation, the extended NR community will have no forward path to acquire these capabilities.

B. There Is Insufficient Spectrum Available for Broadband Applications of the Type Required by First Responders

There is NO spectrum allocated for broadband data applications for Federal and DOD entities. Lucent Technologies estimates *more than 3.1M Federal and Military (North COM) personnel have no dedicated access to broadband spectrum allocations* for mission-critical or public safety and protection activities. "Federal agencies must rely on NTIA to ensure that there is sufficient authorized spectrum to do the job. There is, however, no overarching telecommunication management system in place to address interoperability, harmonization, continuity of government operations through telecommunications, and economies of scale for the federal government."[30] This issue was clearly recognized by Congress last December when it requested the FCC, NTIA and DHS to jointly address the ability of the NR worker to access broadband applications.

While the FCC has allocated 50 MHz at 4.9 GHz for broadband data applications, the value of this spectrum to the NR community is severely limited by its propagation characteristics. Lucent believes that this spectrum is not appropriate to support the deployment of a national network with substantive geographic coverage, but rather is better suited for short-range, "hot-spot" transmission. While the 4.9 GHz allocation does not support the geographic propagation characteristics for a national network, it is unique in that it *is* a broadband spectrum allocation for the traditional public safety community (2.5M estimated users) -- an asset no other *private radio* or *Federal entity* can claim.

IV. THE REPORT TO CONGRESS SHOULD RECOGNIZE THE NEED FOR AN NMBN AND IDENTIFY CERTAIN KEY ELEMENTS

Lucent believes that the Commission's report to Congress should explicitly recognize the need for an NMBN and identify certain key parameters. While many approaches could be adopted to support the needs of the extended NR community, Lucent believes it would be beneficial to identify certain key NMBN elements for Congressional review and offers several additional considerations.

[30] *Spectrum Policy for the 21st Century – The President's Spectrum Policy Initiative: Report 1: Recommendations of the Federal Government Spectrum Task Force*, Department of Commerce, June 2004, *available at*: <http://www.ntia.doc.gov/reports/specpolini/presspecpolini_report1_06242004.pdf> ("*Spectrum Policy Report*").

A. Key Elements of a Dedicated Network

Lucent believes that the key, inseparable elements for the NMBN include: 1) The aggregation of the full NR community into a single user class; 2) the deployment of a single network (most likely comprised of discrete, regional operations); 3) the use of a commercial broadband technology for the platform; and 4) the identification of sufficient spectrum appropriate for broadband applications, in a spectral band that would support a national deployment. Lucent contends that without these four elements, the financial and operational viability of providing this capability is severely compromised.

B. Additional Considerations

♦ Lucent suggests consideration of the creation of a "public safety carrier"; comparable to the "common carrier", but serving all those meeting the user characteristics of the extended NR community. A number of ownership, operational and management approaches could be considered for the "public safety carrier." Lucent notes that the third party provision of public safety services to those that traditionally build and operate their own infrastructures has been considered by a number of public safety organizations in the past[31] and further incentives for considering this approach are referenced in the Presidential Spectrum Direction.

[31] *Fee-for-Service Report*, Public Safety Wireless Network Program, October 2001, *available at*: <http://www.safecomprogram.gov/NR/rdonlyres/B57D45FE-9023-44C1-B950-9386BACB68A6/0/Fee_for_service.pdf>; *Communication Issues for Emergency Communications Beyond E911: Report #1 - Properties and Network Architectures that Communications Between PSAPs and*

- Any national network provided and managed by a "public safety carrier" should be built to the operational characteristics of the public safety users -- including increased geographic coverage, overbuilt capacity, and enhanced redundancy, diversity and reliability.
- To ensure that the public safety carrier does meet the specifications of this extended community, Lucent suggests the creation of a "special purpose authority" that would, at a minimum, set the standards for the deployment and operation of the national network and potentially hold any spectrum on behalf of the NR community.
- The NMBN should be based on commercial 3G wireless technologies. Commercial 3G wireless technologies can provide dedicated and secure broadband wireless communications capabilities to the NR community, which would allow public safety agencies to leverage the existing significant investment in global research and development. Global commercial platforms are compliant with the current and projected data requirements anticipated by the various public safety communities. Further enhancements and extensions to the technology, both within the standard and in support of the standard, will allow commercial technologies to address some of the unique voice needs of the public safety community more efficiently. 3G networks using IP-based open

Emergency Services Personnel Must Meet in the Near Future, Network Reliability and Interoperability Council (NRIC) (Dec. 6, 2004), *available at*: <http://www.nric.org/meetings/docs/meeting_20041206/FG1D%20Final%20Report.pdf>.

standards capabilities like the IP Multimedia Subsystem ("IMS") not only provide the means to share information within the NR community, but can also act as a platform for interoperability with legacy systems, other private networks, and new applications and services.

- There are two major, global commercial standards being used today in the commercial environment—CDMA 2000 and UMTS. Lucent believes that while it is anticipated that there will ultimately be user interoperability across these commercial platforms, any national capability within the next few years should be built to one standard, at least at the outset, to ensure immediate functional interoperability.
- For reasons of practical deployment and operational flexibility, the NMBN could be a network comprised of a number of discrete, non-overlapping regional systems. For example, it has been suggested that the regions could be consistent with FEMA regions to more fully reinforce guidelines associated with the National Response Plan and National Incident Management System. Consistent with the Project MESA[32] approach, while each region could be built consistent with the national guidelines, regional deployment guidelines might be "transposed" to more adequately reflect the specific issues (*e.g.*, topography) associated with that operation.
- Lucent assumes that the NMBN deployment would be more robust in geographic coverage than any single commercial network; however, it

[32] *See* Mesa SoR, *supra* note 9.

may not be practical to cover the entire country. Linking the NMBN with a satellite service (recognizing current capacity limitations may suggest voice-centric connectivity), could provide augmented geographic coverage in non-populated areas.

- The creation of a dedicated mobile broadband network would perform two essential interoperability functions: it can act 1) as a "universal gateway" for all other private, public, evolving wireless (WiFi, Wi-Max, MESH), and satellite networks, and 2) again, employing capabilities like IMS, as a "universal service" layer for the transmission of data and VoIP communications. *Again, the role of this network is not to replace current private voice and/or dispatch networks used by this community. Rather the NMBN is designed to act as a means to provide in-field data access to the "trusted information network."*
- Governments increasingly share many of the same operational imperatives with the commercial environment. As such, *government should take steps now to ensure that the NR Community has access to a secure dedicated broadband network that at a minimum emulates currently available capabilities.* Delays in providing this access will place this community at a mission disadvantage unless they have an access path that is on par with commercial capabilities. This is not to suggest, however, that the operational or security considerations for this community are identical to those delivered to the commercial sector. Rather, by creating a dedicated broadband network tailored to its more stringent

availability, diversity and reliability requirements, this community can benefit from the best of both worlds.

C. Implementation of the NMBN Should Be Accomplished Through Careful Consultation

Lucent believes that there are a number of operational models that could be used in the deployment of the NMBN. Extensive consultation with all relevant and interested parties will be required to ensure that the unique needs and concerns of the extended NR community are given due consideration in the development of a definitive operational model.

D. Spectrum Required for a National Broadband Mobile Network

As outlined previously, no one Federal entity has the authority to implement the changes that would be required to support the creation of this national broadband capability for the NR community. Rather, the obstacles that must be bridged must be done so in a collaborative environment, and codified to a large extent by Congress. Congress clearly recognized these limitations by requesting that this vision be reviewed among the three primary Federal entities whose combined assets could make the most comprehensive recommendation: the FCC, NTIA and DHS.[33]

The creation of any national broadband network for the NR community will open the opportunity for both the FCC and NTIA constituencies to use common spectrum. This approach, while not without precedent, albeit on a smaller scale, would likely represent a significant extension of spectrum policy to date. Pursuit

[33] Intelligence Reform Act § 7502(a).

of this Congressional initiative would be consistent with the Presidential Spectrum Direction[34] and would provide clear evidence of a willingness and ability to take the measures that would promote enhanced interoperability and continuity of government communications.

The Commission's request for comments acknowledges that "not all frequencies are the same"[35] and that one must match "spectrum with appropriate physical characteristics". As noted above, the 50 MHz allocation at 4.9 GHz designated by the FCC for broadband data applications is not appropriate to support the deployment of a national network with substantive geographic coverage.

Public safety spectrum also currently resides in both the upper band of 700 MHz and the recently re-configured 800 MHz band. Lucent notes that the spectrum in the 700MHz band is currently encumbered by broadcast users, though discussions are ongoing about clearing the spectrum for other users, including public safety users. Lucent believes that clearing the 700MHz band by an early date certainly would be a critical step in meeting the needs of the NR community. Lucent also notes that the public safety spectrum in the 700MHz band is not currently channelized to support broadband applications and is designated for wideband data interoperability. It may be possible to re-channelize existing public safety spectrum allocations to support broadband applications, but the decision to: 1) pursue this option; and 2) to share this

[34] *See Spectrum Policy Report, supra* note 30.

[35] Statement of Commissioner Michael J. Copps, *Request for Comments*, *supra* note 1, at 6.

spectrum jointly as an 8-10M NR community, would need to reside with the current public safety community to whom the spectrum is allocated.

1. Relationship of Frequency to Infrastructure Costs

It is axiomatic that the higher the spectral band used to provide a service, the lower the propagation characteristics for any given transmission facility. Therefore, the cost of network implementation is increasingly mitigated as one progresses further down the spectral band. As an example, at 4.9GHz, a national network provider would need to create a transmitter topography that is *3-4 times more dense* than the current 1.8 GHz commercial topography, and *30-34 times more dense* than the current 800 MHz deployments. Costs are further decreased by utilizing commercial technologies compatible with commercial networks and seeking to find ways to leverage the more than 160,000 commercial transmitter sites already located throughout the country. Consequently, to provide cost effective deployment of a national interoperable network, Lucent advocates deploying the NR broadband network at the lowest possible spectrum band available. Lucent is conducting an on-going analysis to determine how many transmitters would be required to provide what we consider a robust geographic footprint for this network at various spectral bands. The analysis attempts to duplicate the current commercial footprint while adding other extensions of existing geographic coverage reflected by current Federal and/or public safety networks, plus additional border coverage where neither commercial nor public safety networks are in place. Lucent anticipates that the DHS-led studies mandated by Congress will be an opportunity to discuss and refine the assumptions concerning this community's coverage requirements in furtherance of assessing the initiative's viability.

2. Amount of Spectrum Required for the NMBN

There are no data-only, IP-only precedents at this time to create a definitive spectrum requirement analysis for the NMBN, but Lucent is conducting on-going analysis to estimate the spectrum requirements for a network that would support 12.5 million NR users. (Note: Lucent has used a higher number than the previously identified 8 –10M user community in order to accommodate future growth.) The Lucent "National Responder" model is built upon a commercial profile, but modified along three key dimensions: 1) The average monthly data usage was increased to 500 Mbytes; 2) the distribution of applications was skewed towards video and large file transfers; and 3) the percentage of users accessing the network during the "busy hour" was increased from 10 to15% (an increase of 50% over commonly accepted traffic engineering practices).

Based on initial results, Lucent Technologies believes that the core needs of the extended NR community, described in Section II.E. above, for interoperable broadband wireless services could be met with 10-15 MHz of spectrum. Lucent expects to refine this analysis through collaboration with the public safety community over the next several months; however, this initial conclusion was reached after careful analysis of available information on the data needs and requirements of the user community in the context of current, commercially available technologies, noting their anticipated (*i.e.*, published) evolution plans. Lucent estimates that the 10-15 MHz of broadband spectrum would not only support this population, but also would provide the capacity to support "over-provisioning" for extraordinary event situations.

Lucent would emphasize that this spectrum estimate is speculative in nature, and this summary analysis is not meant to be definitive. Lucent trusts that the Congressionally dictated DHS studies associated with the deployment, operation and management of a national network will provide the opportunity to discuss at greater length the assumptions that this estimate was based upon. In particular, traffic statistics from the current DC Government broadband trial,[36] as well as the ARJIS trial in San Diego, CA[37] might provide additional insights and provide a clearer means of assessing what the spectrum needs would be for such a capability.

V. CONCLUSION

In summary, creating a dedicated, secure, broadband mobile network will place this constituency on par with commercial capabilities, and provide a fulcrum to create enhanced capabilities and applications.

With the deployment of a NMBN, the extended NR community would have one ubiquitous communications infrastructure capable of acting as a universal transport layer for information sharing, as a gateway to private and public networks and a means of providing connectivity or backhaul for other security-related networks. Through the deployment of a national broadband network, the

[36] *See* Spectrum Coalition for Public Safety, *available at*: <http://www.spectrumcoalition.dc.gov/html/home.html>.

[37] *See* Automated Regional Justice Information System (ARJIS), *available at*: <http://www.arjis.org/>.

extended NR community would have achieved for data- or information-sharing what DHS refers to as Level 6, or "Standards-Based Shared System"[38] interoperability. The deployment of a national network is a large undertaking---but this is an undertaking that *can* be achieved, as evidenced by the successful commercial wireless market and one that can be duplicated for this key constituency, in part because of the private sector's extensive experience in this domain.

/s/ Charles B. Mathias

Charles B. Mathias
Lucent Technologies, Inc.
1100 New York Avenue, NW
640 West Tower
Washington, DC 20005
202 312-5908
cbmathias@lucent.com

April 28, 2005

[38] *See Interoperability Continuum*, *supra* note 29.